REMARKS

A. Claims 1, 10, 19, 28, 34-42, and 51-53 stand rejected under 35 U.S.C. §102(b) as allegedly anticipated by Wechselberger. The rejection is respectfully traversed. The responsive remarks in the final Office Action contend that Claim 1 is found in the Abstract of Wechselberger under a "broadest reasonable interpretation" of Wechselberger. Applicant disagrees, because the Office Action ignores numerous features of the claim that are not fairly found in the Abstract of Wechselberger. For example, a first user exchange key received from a user and a first shared secret key have no role, in the Abstract of Wechselberger, in determining other secret keys. The Office Action improperly characterizes steps of the claim having numerous specific features as merely "computing" steps with nothing more.

Nevertheless, to expedite prosecution, Claim 1 and all other independent claims are amended to incorporate a sub-step of Claim 4. Each of Claims 1, 10, 19, 28, 34-42, and 51-53 incorporates this subject matter, directly or indirectly by dependency. A rejection for anticipation under §102(b) requires the cited reference to disclose each and every element, step or limitation of the rejected claim, and conversely, a claim with even one feature not found in the reference is not anticipated. See *Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 1548, 220 USPQ 193, 198 (Fed. Cir. 1983). The Office Action did not reject Claim 4 or other corresponding claims under §102(b) based on Wechselberger, and cannot, because the subject matter of Claim 4 is not found in Wechselberger. Therefore, Claims 1, 10, 19, 28, 34-42, and 51-53 are not anticipated by Wechselberger. Reconsideration is respectfully requested.

B. Claims 1, 10, 19, 28, 34-42, and 51-53 stand rejected under 35 U.S.C. §102(b) as allegedly anticipated by Hardjono. The rejection is respectfully traversed.

As with Wechselberger, the Office Action ignores features of the claims, and also does not properly interpret FIG. 5 of Hardjono. For example, in Claim 1, for a first user joining the

first multicast group, in the second computing step, a second secret key is computed based on the first user exchange key and the first shared secret key. In stark contrast, in Hardjono FIG. 5, a key server **distributes to** a joining client a new common group key and a new domain key **using** (that is, encrypted using) its current domain key. Nothing in Hardjono teaches **each group member self-computing** a new key based on its prior secret key and group exchange key. "Using" in Hardjono does not mean "based on."

Nevertheless, to expedite prosecution, Claim 1 and all other independent claims are amended to incorporate a sub-step of Claim 4. Each of Claims 1, 10, 19, 28, 34-42, and 51-53 incorporates this subject matter, directly or indirectly by dependency. A rejection for anticipation under §102(b) requires the cited reference to disclose each and every element, step or limitation of the rejected claim, and conversely, a claim with even one feature not found in the reference is not anticipated. See *Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 1548, 220 USPQ 193, 198 (Fed. Cir. 1983). The Office Action did not reject Claim 4 or other corresponding claims under §102(b) based on Hardjono, and cannot, because the subject matter of Claim 4 is not found in Hardjono. Therefore, Claims 1, 10, 19, 28, 34-42, and 51-53 are not anticipated by Hardjono. Reconsideration is respectfully requested.

C. Claims 7, 16, 25, and 48 stand rejected under 35 U.S.C. §103 as allegedly obvious in view of Hardjono. The rejection is respectfully traversed.

Each of Claims 7, 16, 25, and 48 incorporates, by dependency, the subject matter described above for the amended independent claims. Further, the additional "computing" steps recited in Claims 7, 16, 25, and 48 are not taught or suggested by Hardjono under the rationale asserted in the Office Action.

For example, in Claim 7, for a second user joining the second multicast group, in the computing step, a third secret key is computed based on the second user exchange key and the

second shared secret key. In stark contrast, in Hardjono FIG. 5, a key server **distributes to** a joining client a new common group key and a new domain key **using** (that is, encrypted using) its current domain key. Nothing in Hardjono teaches **each group member self-computing** a new key based on its prior secret key and group exchange key. "Using" in Hardjono does not mean "based on."

A careful, searching review of the features of Claim 7 reveals that the approach of the claim is totally different from Hardjono. In an implementation of the claimed method, any new member who would like to join a group simply broadcasts his part of the key to the entire group, and only one of the existing group members has to respond by broadcasting its part of the key. This approach drastically reduces the number of messages that are required for establishing the secret key. There is no need for the new member to get the key values from each and every individual of the group. The entire group does a key exchange with the new member of the group. Instead of each member picking a random integer for Diffie-Hellman exchange, each group member takes the currently established secret key as a random integer (or as a seed for generating a random integer) and performs a Diffie-Hellman exchange with the new member of the group. Thus, they all end up with the same shared secret key.

Hardjono, in contract, represents a different method, in which a centralized key server has to contact each group member and give it a replacement key. The replacement keys are centrally generated and cannot be based on existing group member keys.

Hardjono lacks any suggestion of the claimed method as clarified herein. Therefore, the rejection under §103 is not supported. Reconsideration is respectfully requested.

D. Claims 6, 15, 24, and 47 stand rejected under 35 U.S.C. §103 as allegedly obvious over Hardjono in view of Aziz. The rejection is respectfully traversed.

Each of Claims 6, 15, 24, and 47 indirectly includes, by dependency, the subject matter of the amended independent claims. Thus, even if Aziz suggests the subject matter that is specifically recited in Claims 6, 15, 24, and 47, a combination of Hardjono with Aziz does not disclose, teach or suggest all features that are recited in Claims 6, 15, 24, and 47, for the reasons given above with respect to Claims 1 and 10. Reconsideration is respectfully requested.

E. Claims 2-5, 11-14, 20-23, 29-31, and 43-46 stand rejected under 35 U.S.C. §103 as allegedly obvious over Hardjono in view of Koblitz. The rejection is respectfully traversed.

The Office Action contends that Koblitz teaches the claimed mathematical relationship of various key elements at page 23, referring to performing modular exponentiation by the repeated squaring method. This is incorrect. Koblitz merely teaches a way to find the value of $b^n \bmod m$, but does not teach or suggest anything about what b, n, and m represent. There is no disclosure, teaching or suggestion that b could be a user exchange key value, that n is a first shared secret key, that m could be is a prime number selected by all members of a multicast group, or that the result of the expression could be used as a second secret key, as claimed.

Indeed, Koblitz even can be viewed as teaching away from applicants' approach because Koblitz is a book about number theory as applied to cryptography, yet Koblitz gives no suggestion about any particular application of the least non-negative residue expression. This is because Koblitz focuses solely on *solving* the expression and not its *applications*.

None of the other references suggests applying a non-negative residue expression to the computation, at multicast group members, of new keys. This is because having each group member self-compute a new key when a group member joins, based on one key portion provided by the joining method and another key portion provided by one responding existing group member, so that all group members arrive at the same new key, is completely counter-intuitive.

In prior approaches, centralized key distribution, or individual re-negotiations of new keys among group members, are always used.

For all the foregoing reasons, a combination of Hardjono and Koblitz fail to disclose, teach or suggest the claimed combination. Reconsideration is respectfully requested.

F. Claim 32 stands rejected under 35 U.S.C. §103 as allegedly obvious over Hardjono in view of Aziz and Koblitz. The rejection is respectfully traversed.

Claim 32 indirectly includes, by dependency, the subject matter of the amended independent claims. Hardjono and Koblitz fail to disclose, teach or suggest features of the claims, as described above with respect to Claim 1, which has the same amendment as Claim 29 from which Claim 32 depends, and Claim 4. Thus, even if Aziz suggests the subject matter that is specifically recited in Claim 32, a combination of Hardjono with Aziz and Koblitz does not disclose, teach or suggest all features that are recited in Claim 32, for the reasons given above. Reconsideration is respectfully requested.

G. Claims 9, 18, 27, and 50 stand rejected under 35 U.S.C. §103 as allegedly obvious over Hardjono in view of Srivastava. Further, Claims 8, 17, 26, 33, and 49 stand rejected under 35 U.S.C. §103 as allegedly obvious over Hardjono in view of Koblitz and Srivastava. The rejections are respectfully traversed.

Srivastava is not citable as a prior art reference in this case. Under 35 U.S.C. §103(c), subject matter developed by another person, which qualifies as prior art only under 35 U.S.C. §102(e), (f), or (g), shall not preclude patentability where the subject matter and the claimed invention were, at the time the invention was made, owned by the same person or subject to an obligation of assignment to the same person. The filing date of Srivastava is December 22, 1999 and the issue date is January 27, 2004. The filing date of the present application is June 30, 2000.

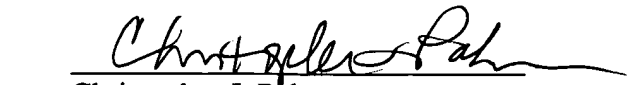
Therefore, Srivastava qualifies as prior art only under 35 U.S.C. §102(e) and not, for example, under 35 U.S.C. §102(b).

The assignee stated on the face page of Srivastava is Cisco Technology, Inc. The assignee of the present application is Cisco Technology, Inc., as stated in the Assignment that has been recorded at Reel 011221, Frame 0090. Thus, both Srivastava and the present application were owned by the same legal person at the time the present application was filed. (Applicants do not admit that their filing date is "the time the invention was made" as recited in 103(c), but to the extent necessary to resolve the issue here, applicants aver that Srivastava and the claimed invention were, at the time the invention was made, owned by or subject to an obligation of assignment to the same legal person.)

All requirements of §103(c) are met, and Srivastava must be removed as a reference. See MPEP 2146. Further, since Srivastava does not qualify as a prior art reference, Srivastava cannot support the rejections under 35 U.S.C. §103. Reconsideration is respectfully requested.

H. A check for applicable extra claim fees and extension fees is enclosed. If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP



Christopher J. Palermo
Reg. No. 42,056

Date: November 11, 2004

1600 Willow Street
San Jose, CA 95125
Telephone: (408) 414-1080, ext. 202
Facsimile: (408) 414-1076